

In the claims:

Please amend the claims as follows:

Claim 1 (currently amended): A method for securing an accessible computer system, the method comprising:

monitoring a computer system for connection transactions between ~~multiple at least one~~ access ~~requestor~~requestors and ~~multiple at least one~~ access ~~provider~~providers using a switching component connected to the multiple access providers; and

B1 denying access by ~~an attacking~~the access requestor to the access ~~provider~~providers when a number of connection transactions initiated by the ~~attacking~~ access requestor ~~through the switching component~~ exceeds a configurable threshold number during a first configurable period of time.

Claim 2 (currently amended): The method as in claim 1, wherein the monitoring includes detecting connection transactions initiated by the access ~~requestor~~requestors ~~through the switching component~~.

Claim 3 (currently amended): The method as in claim 2, wherein the monitoring further includes counting the number of connection transactions initiated by the access ~~requestor~~requestors ~~through the switching component~~ during the first configurable period of time.

Claim 4 (currently amended): The method as in claim 3, wherein the monitoring further includes comparing the number of connection transactions initiated by the access ~~requestor~~requestors ~~through the switching component~~ during the first configurable period of time to the configurable threshold number.

Claim 5 (currently amended): The method as in claim 1, wherein the monitoring includes detecting connection transactions between ~~multiple at least one~~ Internet protocol ~~address~~addresses and the access ~~provider~~providers with the switching component.

Claim 6 (currently amended): The method as in claim 5, wherein the monitoring further includes counting the number of connection transactions initiated through the swithing component by the Internet protocol ~~address~~addresses during the first configurable period of time.

Claim 7 (currently amended): The method as in claim 6, wherein the monitoring further includes comparing the number of connection transactions initiated by the Internet protocol ~~address~~addresses through the switching component during the first configurable period of time to the configurable threshold number.

31
cont
Claim 8 (original): The method as in claim 6, wherein the monitoring includes monitoring a computer system for connection transactions made using TCP.

Claim 9 (currently amended): The method as in claim 5, wherein the detecting includes identifying the Internet protocol ~~address~~addresses through the use of a header attached to a message representing the connection transaction being detected.

Claim 10 (currently amended): The method as in claim 1, wherein the denying of access includes denying access to the access ~~provider~~providers through the switching component by the attacking access requestor for a second configurable period of time.

Claim 11 (currently amended): The method as in claim 10, wherein the denying of access further includes resetting the second configurable period of time after detecting a new connection transaction initiated by the attacking access requestor through the switching component during the second configurable period of time.

Claim 12 (currently amended): The method as in claim 1, wherein the denying of access includes denying access to the access ~~provider~~providers through the switching component by the attacking access requestor for a second configurable period of time after detecting a most recent

connection transaction initiated by the attacking access requestor through the switching component.

Claim 13 (currently amended): The method as in claim 1, wherein the access ~~requestor~~requestors ~~are~~is a ~~client~~clients and the access ~~provider~~providers ~~are~~is a ~~host~~hosts such that the monitoring includes detecting connection transactions through the switching component between ~~multiple~~at least one ~~client~~clients and ~~multiple~~at least one ~~host~~hosts.

Claim 14 (currently amended): The method as in claim ~~3~~1, wherein the counting further comprises counting a cumulative number of connection transactions for the multiple access providers connected to the switching component initiated by each of the access requestors during the first configurable period of time. ~~access requestor is a client and the access provider is a host such that the monitoring includes detecting connection transactions between the access requestor and a plurality of access providers.~~

Claim 15 (currently amended): A system for securing an accessible computer system, comprising:

means for a switching component connected to multiple access providers to:
monitoring a computer system for connection transactions between ~~multiple~~at least one access ~~requestor~~requestors and ~~the multiple~~at least one access ~~provider~~providers; and
~~means for denying access by an attacking~~the access requestor to the access ~~provider~~providers when a number of connection transactions initiated by the attacking access requestor ~~exceed~~exceeds a configurable threshold number during a first configurable period of time.

Claim 16 (currently amended): The system of claim 15, wherein the means for ~~monitoring the switching component~~ includes:

means for detecting connection transactions initiated by the access ~~requestor~~requestors through the switching component;

means for counting the number of connection transactions initiated by the access requester ~~requestors~~ through the switching component during the first configurable period of time; and

means for comparing the number of connection transactions initiated by the access requester ~~requestors~~ through the switching component during the first configurable period of time to the configurable threshold number.

Claim 17 (currently amended): The system of claim 15, wherein the means for ~~monitoring~~ the switching component includes:

means for detecting connection transactions between ~~multiple at least one~~ Internet protocol ~~address~~ addresses and the access ~~provider~~ providers using the switching component;

means for counting the number of connection transactions initiated by the Internet protocol ~~address~~ addresses through the switching component during the first configurable period of time; and

means for comparing the number of connection transactions initiated by the Internet protocol ~~address~~ addresses through the switching component during the first configurable period of time to the configurable threshold number.

Claim 18 (original): The system of claim 17, wherein the means for monitoring includes means for monitoring a computer system for connection transactions made using TCP.

Claim 19 (currently amended): The system of claim 17, wherein the means for detecting includes:

means for identifying the Internet protocol ~~address~~ addresses through the use of a header attached to a message representing the connection transaction being detected.

Claim 20 (currently amended): The system of claim 15, wherein the means for ~~denying access~~ the switching component includes:


means for denying access to the access ~~provider~~ providers through the switching component by the attacking access requestor for a second configurable period of time.

Claim 21 (currently amended): The system of claim 20, wherein the means for denying access further includes:

means for resetting the second configurable period of time after detecting a new connection transaction initiated by the attacking access requestor through the switching component during the second configurable period of time.

Claim 22 (currently amended): The system of claim 15, wherein the means for ~~denying access~~the switching component includes:

means for denying access to the access ~~provider~~providers through the switching component by the attacking access requestor for a second configurable period of time after detecting a most recent connection transaction initiated by the access requestor.

 Claim 23 (currently amended): The system of claim 15, wherein the access ~~requestor~~requestors are ~~a client~~clients and the access ~~provider~~providers are ~~a host~~hosts such that the means for ~~monitoring~~the switching component includes:

means for detecting connection transactions through the switching component between multiple at least one client~~clients~~ and multiple at least one host~~hosts~~.

Claim 24 (currently amended): The system of claim ~~15~~16, wherein the means for counting further comprises means for counting a cumulative number of connection transactions for the multiple access providers connected to the switching component initiated by each of the access requestors during the first configurable period of time. ~~access requestor is a client and the access provider is a host such that the means for monitoring includes:~~

~~means for detecting connection transactions between the access requestor and a plurality of access providers.~~

Claim 25 (currently amended): A system for securing an accessible computer system, comprising:

a switching component connected to multiple access providers to:

~~a monitoring component that is structured and arranged to monitor a computer system for connection transactions between multipleat least one access requesterrequestors and multipleat least one access providerproviders; and~~

~~a blocking component that is structured and arranged to deny access by the access requestor to the access providerproviders when a number of connection transactions initiated by an attackingthe access requestor exceed a configurable threshold number during a first configurable period of time.~~

Claim 26 (currently amended): The system of claim 25, wherein the ~~monitoring~~switching component comprises:

a detection component that is structured and arranged to detect connection transactions initiated by the access ~~requestor~~requestors through the switching component;

a counting component that is structured and arranged to count the number of connection transactions initiated by the access ~~requestor~~requestors through the switching component during the first configurable period of time; and

a comparing component that is structured and arranged to compare the number of connection transactions initiated by the access ~~requestor~~requestors through the switching component during the first configurable period of time to the configurable threshold number.

Claim 27 (currently amended): The system of claim 25, wherein the ~~monitoring~~switching component comprises:

a detection component that is structured and arranged to detect connection transactions through the switching component between multipleat least one Internet protocol addressaddresses and the access ~~provider~~providers;

a counting component that is structured and arranged to count the number of connection transactions initiated through the switching component by the Internet protocol ~~address~~addresses during the first configurable period of time; and

a comparing component that is structured and arranged to compare the number of connection transactions initiated through the switching component by the Internet protocol

B1
cont

~~address~~addresses during the first configurable period of time to the configurable threshold number.

Claim 28 (original): The system of claim 27, wherein the connection transactions include connections made using TCP.

Claim 29 (currently amended): The system of claim 27, wherein the detection component comprises:

an identifying component that is structured and arranged to identify the Internet protocol ~~address~~addresses through the use of a header attached to a message representing the connection transaction being detected.

Claim 30 (currently amended): The system of claim 25, wherein the ~~blocking~~switching component comprises:

an access preventer that is structured and arranged to deny access to the access ~~provider~~providers through the switching component by the attacking access requestor for a second configurable period of time.

Claim 31 (currently amended): The system of claim 30, wherein the ~~blocking~~switching component further comprises:

a timing component that is structured and arranged to measure the second configurable period of time during which the access preventer denies access to the access ~~provider~~providers by the attacking access requestor.

Claim 32 (currently amended): The system of claim 31, wherein the ~~blocking~~switching component further comprises:

a reset component that is structured and arranged to reset the timing component after detecting a new connection transaction initiated by the attacking access requestor through the switching component during the second configurable period of time.

Claim 33 (currently amended): The system of claim 25, wherein the ~~blocking~~switching component comprises:

an access preventer that is structured and arranged to deny access to the access ~~provider~~providers through the switching component by the attacking access requestor for a second configurable period of time after detecting a most recent connection transaction initiated by the access requestor.

Claim 34 (currently amended): The system of claim 25, wherein the access ~~requestor~~requestors are-is-a clientclients and the access ~~provider~~providers are-is-a hosthosts such that the ~~monitoring~~switching component comprises:

a detection component that is structured and arranged to detect connection transactions through the switching component between multiple~~at least one~~ clientclients and multiple~~at least one~~ hosthosts.

137
cont
Claim 35 (currently amended): The system of claim ~~25~~26, wherein the counting component further comprises counting a cumulative number of connection transactions for the multiple access providers connected to the switching component initiated by each of the access requestors during the first configurable period of time~~access requestor is a client and the access provider is a host such that the monitoring component comprises:~~

~~—— a detection component that is structured and arranged to detect connection transactions between the access requestor and a plurality of access providers.~~

Claim 36 (currently amended): The system of claim 25, wherein ~~the monitoring component and the blocking component are included in~~ a host computer system that receives communications from at the switching component.

Claim 37 (currently amended): The system of claim 25, wherein the ~~monitoring component and the blocking~~switching component ~~are~~is included in a switch that receives communications ~~from a host computer system~~.